Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Policies and Rules	)	CC Docket No. 93-292
Concerning Toll Fraud	)	

COMMENTS OF
THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Michael F. Altschul
Cellular Telecommunications
Industry Association
1133 21 Street. N.W.
Third Floor
Washington, D.C. 20036
(202) 785-0081

DATED: January 14, 1994

Summary

Fraud is costing the cellular industry approximately one million dollars a day. CTIA endorses the Commission's proposal to combat cellular fraud by strengthening the wording of Rule 22.915 to insure that each mobile unit maintains the integrity of a unique factory set Electronic Serial Number. In addition, the Commission should urge Congress to enact new legislation that would make altering an ESN a federal crime, and the Commission should work with the industry in asking Congress to give federal law enforcement agencies the tools they need to prosecute cellular fraud by modifying 18 U.S.C. Section 1029, the federal criminal statute that makes it a crime to use a counterfeit access device to commit fraud. Finally, CTIA agrees with the Commission that liability for fraud should rest with the entity most able to control it.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Policies and Rules	)	CC Docket No. 93-292
Concerning Toll Fraud	)	

COMMENTS OF
THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Cellular Telecommunications Industry Association ("CTIA") hereby submits its comments on the Notice of Proposed Rule Making in the above-captioned proceeding.[1/] CTIA is a trade association whose members provide Commercial Mobile Services, including over 95 percent of the licensees providing cellular service to the United States, Canada, and Mexico, and the nation's largest providers of ESMR service. CTIA's membership also includes wireless equipment manufacturers, support service providers, and others with an interest in the wireless industry. CTIA and its members have a direct and vital interest in the outcome of this proceeding.

Introduction

In this docket, the Commission has proposed policies and rules regarding toll fraud. With respect to cellular fraud, the Commission has asked for comment on: 1) its proposed rule to help reduce cellular fraud caused by tampering with a mobile unit's

---

[1/] In the Matter of Policies and Rules Concerning Toll Fraud, Notice of Proposed Rule Making, CC Docket No. 93-292 FCC 93-496, 8 FCC Rcd [ ] (released Dec. 2, 1993)("Notice").

unique Electronic Serial Number ("ESN")[2/]; 2) what further efforts on the part of the Commission and the institutions fighting cellular fraud would aid in combatting fraud; and 3) how issues like those raised in the context of CPE-based fraud should be resolved in the context of cellular fraud. In response, CTIA again endorses the proposal to strengthen the wording of Rule 22.915 originally set forth in the Commission's Part 22 rewrite proceeding, Revision of Part 22 of the Commission's Rules Governing the Public Mobile Service, Notice of Proposed Rulemaking, 7 FCC Rcd 3658, 3741 (1992); in addition, the Commission should go further and urge Congress to enact new legislation that would make altering an ESN a federal crime, and the Commission should work with the industry in asking Congress to give federal law enforcement agencies the tools they need to prosecute cellular fraud by modifying 18 U.S.C. Section 1029, the federal criminal statute that makes it a crime to use a counterfeit access device to commit fraud. Finally, CTIA agrees with the Commission that liability for fraud should rest with the entity most able to control it.

The Commission is absolutely correct when it states that "both customers and carriers suffer the effects of fraud." Notice at ¶ 4. CTIA estimates that U.S. and Canadian cellular carriers lost nearly $300 million to fraud in 1992. At present,

---

[2/]The ESN is a 32 bit binary number that uniquely identifies a mobile station to any cellular system for billing and other purposes.

the industry estimates that it is losing between $300 to $400 million a year, or approximately $1 million a day to fraud.

Unlike certain victims of "toll fraud" or "PBX fraud",[3] cellular carriers do not look to their customers to recover charges associated with fraudulent calls. However, because cellular carriers are required to pay both interexchange and local exchange carriers for completing uncollectible fraudulent calls, cellular carriers, and ultimately their customers, assume these costs. The Commission is therefore correct when it observes that "[t]he fraudulent use of cellular telephones has become a serious industry problem that results in financial losses to consumers, and increases the cost of doing business for the cellular industry." Notice at ¶ 32.

In 1991, in response to the industry's growing exposure to fraud, CTIA launched a full-time program to combat cellular fraud.[4] The association's Fraud Task Force concentrates on field investigations to gather information about fraud trends, training programs to educate carriers and law enforcement

---

[3] See, for example, Chartways Technologies, Inc. v. AT&T Communications, Memorandum Opinion and Order, FCC 93-994 (released August 19, 1993).

[4] Because cellular carriers do not require legitimate customers to pay for fraudulent calls billed to their account, cellular carriers have a $300 million a year incentive to develop anti-fraud solutions. The Commission can assist the industry along the lines proposed in these comments and in the comments of other wireless providers, but the Commission need not charter new initiatives to provide the industry with additional incentives to combat fraud. See Notice at ¶ 34.

agencies, and technology research to examine technical and operational solutions.

CTIA member carriers meet regularly through Fraud Task Force meetings, workshops, and training programs to share information about fraud trends, and prevention techniques. From investigations into subscription, tumbling, and cloning fraud, over 200 suspects have been arrested and over 500 counterfeit phones and thousands of computer chips have been seized. CTIA estimates that its anti-fraud activities have resulted in a total loss avoidance of over $100 million. Through the multi-media *Train the Trainer* program, nearly 120 carriers and over 6,000 employees were given cellular fraud prevention training. The law enforcement training program has substantially raised the level of awareness of over 1,600 officers from 250 federal and local agencies, the product of which has lead to greater cooperation between carriers and law enforcement.

I. Unique Unit Identification Is Essential to the Success of Wireless Services; the Commission's Rules and Enforcement Activity Should Insure that Each Mobile Unit Is Uniquely Identified

As the Notice observes, the three major types of cellular fraud are subscription fraud,[5] stolen phone fraud,[6] and access

---

[5] Subscription fraud occurs when someone subscribes to cellular service with false information and no intention to pay for service. Carriers are defrauded when they provide service through the initial billing cycle, and are unable to collect from the fraudulent customer.

[6] Stolen phone fraud involves the unauthorized use of a phone stolen from a legitimate customer before that customer can report the theft.

fraud. Notice at ¶ 33. Because the Commission is not charged with enforcing criminal statutes, both subscription fraud and stolen phone fraud are outside of the FCC's jurisdiction.[7/] The Commission does, however, have the authority to address access fraud by tightening its rules that require each mobile transmitter to have a unique ESN.

To have viable commercial mobile services, it is essential that all mobile units have a unique identification number.[8/] Protecting the integrity of each mobile unit's unique ESN provides cellular and other wireless carriers with the ability to establish validation processes for the provision of service to subscribers. Effective validation is necessary to bill customers for their use of wireless services, and is essential in combatting access fraud, since cellular systems sort legitimate users from illegitimate users based on a mobile unit's ESN. Finally, without effective validation processes, carriers are not able to provide Court-authorized surveillance on behalf of law enforcement agencies. Without the ability to uniquely identify a mobile unit, carriers cannot determine the location or identity of surveillance targets.

[7/]The Commission's jurisdiction relates to interstate and foreign communications by wire or radio. See Communications Act of 1934, 47 U.S.C. § 152. The Department of Justice and local law enforcement agencies are charged with the enforcement of criminal statutes. Notice at ¶ 6.

[8/]In addition to the ESN, which uniquely identifies a mobile unit, cellular phones also are identified by a Mobile Identification Number, which is a 24 bit number that corresponds to the telephone number assigned to the customer.

The Commission's rules have long recognized the importance of maintaining the integrity of each mobile unit's ESN. The Commission's technical rules for cellular service require that the ESN "be factory-set and not readily alterable in the field. The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative." OET Bulletin No. 53.[9] As the Notice observes, the FCC has proposed revising this language to more precisely address ESN integrity.[10]

---

[9]OET Bulletin No. 53 is contained in Appendix D to the Report and Order in CC Docket No. 79-318.

[10]In Revision of Part 22 of the Commission's Rules Governing the Public Mobile Service, Notice of Proposed Rulemaking, 7 FCC Rcd 3658, 3741 (1992), the Commission proposed a new rule establishing additional technical specifications to prevent tampering with a mobile unit's ESN.

Proposed Section 22.919 provides that each mobile transmitter must have a unique ESN that must be factory set, and must not be alterable, removable or otherwise able to be manipulated in the field. The proposed rule also requires that the ESN host component must be permanently attached to a main circuit board and the integrity of the mobile unit's operating software must not be alterable. Finally, the cellular equipment must be designed so that any attempt to remove, tamper with, or change the ESN chip, its logic system, or firmware originally programmed by the manufacturer will render the mobile transmitter inoperative.

CTIA has endorsed proposed Section 22.919, calling it "an excellent proposal that will assist carriers to secure their systems against fraud." CTIA Comments, CC Docket No. 92-115 (Oct. 5, 1992) at 7-8. However, we did suggest that § 22.919(a) be altered to read that ESN manipulation should not be possible "outside a manufacturer's authorized facility" to make clear that factory authorized service centers may complete legitimate repairs. Id. at 8.

In addition to adopting language to tighten the technical rules that require each mobile transmitter to have a unique ESN, the Commission also should strengthen its enforcement activities. The Commission has stated that "[i]t is a violation of Section 22.915 of the Commission's Rules for an individual or company to alter or copy the ESN of a cellular telephone. Moreover, it is a violation of the Commission's rules to operate a cellular telephone that contains an altered or copied ESN."[11/] Letter from John Cimko, Chief, Mobile Services Division, to Michael Altschul, CTIA (Jan. 15. 1993).

Under Section 22.120 of the Rules, all cellular phones (in fact, all "transmitters" operated in common carrier mobiles services) must be type-accepted by the Commission. Section 22.120(d) of the Rules expressly provide that:

> "*Cellular equipment*. In addition to the normal type-acceptance procedures contained in Part 2 of [the technical rules], transmitters designed for operation under [the cellular rules] shall comply with the requirements contained in the Commission's cellular system compatibility specifications (See § 22.915)."

Section 22.120, (49 FR 3334, Jan.26 1984).

Read together, it is clear that continuing compliance with the cellular compatibility specifications is a prerequisite to the effectiveness of a grant of type acceptance to a cellular

---

[11/] See also, Public Notice, "Changing Electronic Serial Numbers on Cellular Phones Is a Violation of the Commission's Rules," Rpt. No. CL-52-3 (Oct. 2, 1991)("Phones with altered ESNs do not comply with the Commission's rules and any individual or company operating such phones or performing such alterations is in violation of Section 22.915 of the Commission's rules and could be subject to appropriate enforcement action.").

mobile unit, and that any party who modifies an ESN so that the phone no longer complies with Section 22.915 of the Rules is violating the Commission's Equipment Authorizations program.[12/]

CTIA urges the Commission to utilize its Equipment Authorizations Program as an enforcement mechanism to combat the use of devices and software that are used to alter the factory set ESN of cellular mobile units. In this regard, CTIA endorses the proposal suggested in the Notice that the Commission exercise its Section 503(b)(5) authority to institute forfeiture proceedings against non-licensees or non-applicants who willfully or repeatedly violate the Commission's rules.

[12/]Section 2.1001 of the Rules permits only two classes of permissive changes to be made in type accepted equipment without the filing of an entirely new application by, and grant of type acceptance to, the party making the change. Class I permissive changes (§ 2.1001(b)(1)) are generally those of a cosmetic nature which do not change the equipment's technical performance, while Class II permissive changes (§ 2.1001(b)(2)) change either the technical characteristics or performance of the equipment as originally reported and may be made only so long as the device continues to perform within the Commission's regulatory limits, and only after the changes have been reported to and approved by the Commission prior to marketing.

Given the requirements of Section 22.120(d) and the statement in the letter from John Cimko to Michael Altschul that changes to an ESN would violate these requirements, it is clear that any party who changes the ESN of a cellular mobile unit has made a change that is not permitted by Section 2.1001 of the Rules.

Note, however, that under Section 2.1001(b)(3), factory or licensee authorized technicians are permitted to replace the factory set ESNs in the course of repairing a subscriber's phone, since this would be a change made on behalf the grantee. This limited circumstance is quite different from software or firmware changes made by a third party or user without authorization from the grantee that brings the phone out of the manufacturer's specifications by altering the unit's factory set ESN.

II. The Commission Should Ask Congress to Pass New Legislation to Make Altering an ESN or Using a Mobile Unit with an Altered ESN a Crime

The Notice requests comment as to whether "unique criminal legislation is necessary." Notice at ¶ 34. CTIA believes that the Commission should pursue legislation both to make altering an ESN a crime, and to enhance the ability of federal law enforcement agencies to investigate and prosecute cellular fraud.

The statutory provision usually relied upon to prosecute toll fraud in Federal court is 18 U.S.C. § 1029, which makes it a crime to "knowingly and with intent to defraud" use, produce or traffic in one or more "counterfeit access devices." As the record in the Commission's October 9, 1992 en banc hearing on Toll Fraud established, some federal courts have interpreted this statute to require proof that a person's account has been fraudulently accessed. In many toll fraud cases, and especially in cellular access fraud cases, either no "person's" account (i.e., the account of a legitimate subscriber) is accessed, or even when a legitimate subscriber's account is accessed, it may be difficult for a prosecutor to establish "beyond a reasonable doubt" the link between the use of the fraudulent access device and the posting of the charges associated with the fraudulent activity to a legitimate subscriber's account (oftentimes the billing is done by a provider whose network and services are not affiliated, except through a billing agreement, with the network that was fraudulently accessed). See generally, Notice at ¶ 12.

Congress enacted the Counterfeit Access Device statute in 1984, out of concern over "fraudulent use of access devices in connection with credit transactions." United States v. McNutt, 908 F.2d 561, 563 (10th Cir. 1990); see also, 1984 U.S. Code Cong. and Adm. News, 3182. While the statutory language has been interpreted to include "long distance telephone service access codes,"[13] the Court's have been unwilling to extend the scope of the statutory prohibition to reach cellular access fraud.[14] The telecommunications industry and its customers would be best served by statutes that clearly render toll and cellular fraud activities criminal violations subject to straightforward prosecutions at the federal level.[15]

---

[13] See United States v. Teehee, 893 F.2d 271, 272 (10th Cir. 1990).

[14] The Tenth Circuit Court of Appeals recently ruled that Section 1029 does not apply to cellular "tumbling" fraud in the first appellate case interpreting the statute's applicability to cellular access fraud. United States v. Brady, No. 93-4085, slip op. at 13-14 (Dec. 21, 1993)("Although Congress, without question, has the power to criminalize the use of or trafficking in cellular telephones altered to allow free riding on the cellular telephone system, even when such telephones do not access valid identifiable accounts, Congress did not do so when it enacted § 1029").

[15] The Commission also should urge state legislators to make toll fraud and cellular fraud state criminal offenses. The Notice observes that "[t]he Secret Service estimates that as few as thirteen states have enacted statutes specifically dealing with telephone fraud crimes." Notice at n.28.

Legislation recently has been passed in Virginia (adding § 18.2 sections 190.1 through 190.4 to the Code of Virginia), New York (adding Article 157 to Title J of the Penal Law), and California (adding Section 502.8 to the Penal Code and Section 2892.3 to the Public Utilities Code), that specifically addresses cellular fraud. Collectively, these statutes provide model

(continued...)

Legislation is also needed that would make it a crime to alter a mobile unit's ESN in a way that violates the Commission's rules. Such a statute could be modeled on 18 U.S.C. Section 511, which makes it a crime to knowingly remove, obliterate, tamper with or alter a motor vehicle's identification number. Adding the crime of ESN alteration to Chapter 18 of the U.S. Code would permit prosecution of anyone who intentionally removes or alters the ESN of a wireless device in violation of the Commission's rules; it would not require a prosecutor to prove that a person had a specific intent to defraud, or require a prosecutor to trace a fraudulent call to a legitimate customer's account. See generally, United States v. Enochs, 857 F2d 491 (8th Cir. 1988)(18 U.S.C. §511 does not require proof that defendant had specific intent to violate statute when he removed a vehicle identification number from the front end of a car).

In addition to the specific legislation described above, the Commission also should consult with law enforcement agencies and carriers to determine whether legislation is needed to facilitate inter-carrier cooperation in investigating possible toll fraud activities. Carriers might be able to respond more effectively to lawful requests for assistance and information if Congress clarified carriers' ability to receive and share information

---

[15/](...continued)
legislation for those states that have not enacted cellular access fraud laws.

without interfering with the legitimate privacy rights of subscribers.[16]

III. Shared Liability Is Appropriate for Cellular Fraud

CTIA agrees with the Commission that liability for fraud should rest with the entity most able to control it. In a multi-carrier environment where the risk of fraud is shared, the Commission should make a carrier responsible for the fraudulent activity that carrier can control, at least theoretically, or where the carrier has a direct relationship with the user.

Existing arrangements in the cellular industry already reflect this basic theory. Since some cellular carriers provide customers with "equal access", while others resell interexchange service, the allocation of fraudulent losses depends on how long distance service is furnished.

In an equal access environment, a cellular customer selects an interexchange carrier to carry calls that terminate outside of the cellular carrier's local service area. Under this serving arrangement, the cellular carrier must honor the customer's selection of a long distance provider and may not interfere with the customer's business relationship with that carrier. In addition, both the serving cellular carrier and the long distance

---

[16] Cellular carriers are very sensitive to the privacy rights of their subscribers. Carriers often require a subpoena before disclosing information about a customer's telephone number, usage, or other specific information. These practices limit cooperation with other carriers and hinder successful detection and prosecution of fraudulent activities. The Commission should urge all carriers to cooperate to the maximum extent permitted by law in the collection and analysis of information.

company can validate each call. Accordingly, if there is fraudulent calling, the long distance losses should be borne by the interexchange carrier, while cellular air time charges are absorbed by the cellular carrier.

In contrast, where a cellular carrier resells interexchange services to its customers, the interexchange carrier has no opportunity to validate the interexchange portion of the call. In this case, only the cellular carrier is able to validate the call. In this kind of environment, the cellular carrier absorbs both the airtime usage as well as the interexchange service charges assessed by the long distance carrier.

The Commission should preserve existing shared liability arrangements, and extend the principle wherever feasible. A federal policy of shared fraud liability will provide customers and carriers whose facilities and equipment are involved in handling a fraudulent call with a strong incentive to deploy anti-fraud measures and to take other appropriate steps to ensure that fraud is minimized.

In addition, wide-spread adoption of shared liability principles will increase the incentives of carriers to undertake cooperative investigations. In that event, such investigations would no longer aid only interconnected service providers but might also serve to reduce a carrier's own financial exposure.

Finally, while labeling requirements similar to those proposed for Part 68 devices are inappropriate for cellular

mobile units,[17] in the future, cellular carriers will be able to offer customers anti-fraud features such as authentication, Personal Identification Number ("PIN") access codes, and feature restrictions. Customers who have been educated about these features, yet chose to not use them, should be liable for fraudulent use of their account just as the Commission has extended liability for fraud to PBX customers who have elected to not deploy anti-fraud technologies.[18]

---

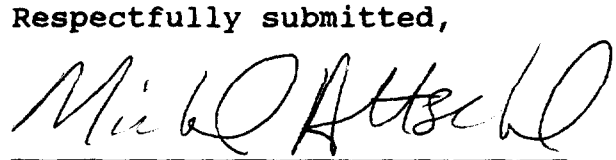
[17]The Commission previously has determined that a rule requiring privacy warning labels for cellular telephones was not in the public interest. Washington Legal Foundation, RM-5577, 2 FCC Rcd 4311 (July 17, 1987).

[18]See Chartways Technologies, Inc. v. AT&T Communications, Memorandum Opinion and Order, FCC 93-994 (released August 19, 1993).

Conclusion

CTIA urges the Commission to adopt stronger anti-fraud measures by strengthening the wording of Rule 22.915. In addition, the Commission should urge Congress to enact new legislation that would make altering an ESN a federal crime, and the Commission should work with the industry in asking Congress to give federal law enforcement agencies the tools they need to prosecute cellular fraud by modifying 18 U.S.C. Section 1029 to explicitly include fraud caused by wireless access devices. Finally, CTIA agrees with the Commission that liability for fraud should rest with the entity most able to control it.

Respectfully submitted,



Michael F. Altschul
Cellular Telecommunications
Industry Association
1133 21 Street. N.W.
Third Floor
Washington, D.C. 20036
(202) 785-0081

DATED: January 14, 1994

Certificate of Service

I, Michael F. Altschul, hereby certify that on this 14th day of January, 1992, copies of the foregoing Comments of the Cellular Telecommunications Industry Association were served by hand delivery upon the following parties:

William Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

International Transcription Service
1919 M Street, N.W., Room 246
Washington, D.C. 20554

Michael F. Altschul